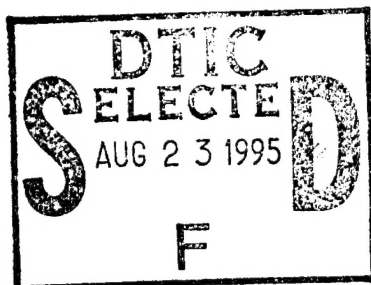


Unclassified



NAVAL WAR COLLEGE
Newport, R.I.

Netwar, It's Not Just For Hackers Anymore

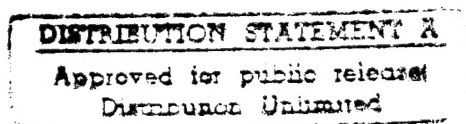
by

Stefan Eisen Jr.

Lt. Col., USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.



Signature: Stefan Eisen Jr.

22 June 1995

Paper Directed By Captain D. Watson
Chairman, Joint Military Operations Department

EK Nielsen
Faculty Advisor

11 May 95
Date

Captain Eugene K. Nielsen, USN
Faculty, Joint Military Operation Department
Adm. Raymond A. Spruance Chair of C4I

UNCLASSIFIED

19950822 042

UNCLASSIFIED

Security Classification This Page

REPORT DOCUMENTATION PAGE

| | | | |
|---|-----------------|--|------------|
| 1. Report Security Classification: Unclassified | | | |
| 2. Security Classification Authority: | | | |
| 3. Declassification/Downgrading Schedule: | | | |
| 4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED | | | |
| 5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT | | | |
| 6. Office Symbol: C | | 7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, R.I. 02841-1207 | |
| 8. Title (Include Security Classification): NETWORK WARFARE: IT'S NOT JUST FOR HACKERS ANYMORE (UNCLASSIFIED) | | | |
| 9. Personal Authors: LT COL STEFAN EISEN JR., USAF | | | |
| 10. Type of Report: FINAL | | 11. Date of Report: 16 MAY 1995 | |
| 12. Page Count: 24 | | | |
| 13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy. | | | |
| 14. Ten key words that relate to your paper: Computer Network Warfare, Information Warfare, Command and Control Warfare | | | |
| 15. Abstract: Network warfare (Netwar) is the latest tool in the Information Warfare toolbox. Where C2W targets the enemy's military electronic spectrum and provides defense against enemy C2W efforts, Netwar targets enemy computer networks that support both military and civilian functions (such as communications, logistics, transportation, and other computer controlled networks) in order to provide the operational commander with an additional tool to either prevent or win conflicts. Netwar also has defensive features, helping the operational commander defend against the inevitable enemy attack on friendly computer network systems. | | | |
| 16. Distribution / Availability of Abstract: | Unclassified XX | Same As Rpt | DTIC Users |
| 18. Abstract Security Classification: UNCLASSIFIED | | | |
| 19. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT | | | |
| 20. Telephone: 841-6457 | | 21. Office Symbol: C | |

Security Classification of This Page Unclassified

| | |
|---------------------|-------------------------------------|
| Accession For | |
| NTIS CRA&I | <input checked="" type="checkbox"/> |
| DTIC TAB | <input type="checkbox"/> |
| Unannounced | <input type="checkbox"/> |
| Justification | |
| By | |
| Distribution / | |
| Availability Codes | |
| Dist | Avail and/or Special |
| A-1 | |

DTIC QUALITY INSPECTED 2,

ABSTRACT

Information Warfare (IW) doctrine is experiencing tremendous growth partially as a result of its spectacular performance in Desert Storm. Supporting IW in Desert Storm, Command and Control Warfare (C2W) strategy helped lead the way to success. However, coalition achievements were due in part to Iraq's lack of understanding of C2W. Future operational commanders must not only tackle the expanding role of C2W, but should use IW's latest tool, Network Warfare (Netwar) to their advantage. Netwar compliments C2W, because it augments the commander's offensive toolbox while expanding C2W's defensive strategy. While offensive C2W primarily targets the enemy's military electronic spectrum, offensive Netwar targets the enemy's military/civilian computer controlled networks and information systems. The power to affect these networks isn't a panacea leading to "bloodless" conflict, but it can give the commander a significant force enhancer. As the most recent arrival on the "electronic" battlefield, Netwar not only provides the commander with several offensive options (from physical destruction to degrading system performance to favorably affecting output information), it reinforces defensive C2W by emphasizing the breadth and depth of today's modern military dependence on computer networks while providing defensive strategy options which compliment and expand existing C2W defensive strategy.

Commanders must realize that using some of the Netwar options detailed in this paper require coordination and approval from senior command authorities, perhaps as high as the NCA. However, planning for these effective options is a direct responsibility of the commander. Thoughtful planning will reveal not only the value of Netwar, but it will highlight equipment, training, strategy and policy shortfalls that must be met by either supporting CINCs or other agencies. Failure to plan and execute effective offensive and defensive Netwar, in both peace and wartime, may give an opponent using Netwar the potential to significantly enhance their forces while taking away an effective force multiplier from the friendly commander.

Network Warfare: It's Not Just For Hackers Anymore

Introduction

"A General who...campaigns...in a...populated country, and has no information, is ignorant of his calling."
Napoleon Bonapart

Knowledge, and the desire to control it, is not new to warfare. Though analysts hail Desert Storm as the first "information war", in reality, information exploitation is easily traced back to the Mongols. They controlled the enemy by feeding them false information about the disposition of their forces. For example, in Khwarizm (an area approximated by today's Iran), the ruler Muhammad Ali Shah was so confused by the Mongol's control of troop information that he fled without a fight--allowing the Mongols to achieve victory by default.¹ From Hannibal, to Napoleon, to Eisenhower, history constantly highlights the commander who understands the power of information.² But Desert Storm is not just another example of information control effectively applied to warfare, it is a watershed event because of the prominent role Information Warfare (IW) held among the other facets of warfare (air, land, sea, and space power). Desert Storm senior commanders were surprised by their dependence on networked computer systems.³ This "surprise" was simply commanders carrying the war to a new high ground--gaining not only air, land, sea, and space superiority, but information superiority. Indeed, experts posit that IW had such a huge impact on Desert Storm it should be recognized as a fifth facet of warfare.⁴ What made Desert Storm such a watershed for IW? The answer lies in a silicon chip the size of a quarter.

This paper intentionally focuses only on Network Warfare (Netwar), a subset of IW. Netwar is a logical next step in the expanding scope of IW concepts. This paper emphasizes the potential of this tool, using IW examples as a basis while exploring potential options this tool gives the commander. Operational commanders must comprehend Netwar, and use it as an offensive "weapon" while preparing defenses against enemy attacks. Without effective Netwar, the commander denies friendly troops a great force multiplier while unnecessarily exposing those same troops to unneeded risks.

Background

"Desert Storm was where an ounce of silicon...may have had more effect than a ton of uranium."

Col. Alan D. Campen, USA, Ret.

The growth of IW and its supporting Command and Control Warfare (C2W) strategy is based on a simple concept: the commander's need to increase the power of friendly assets while denying the enemy the same. One answer to this "need" is manipulating information. Before electronics, information was physically recorded or memorized and then relayed to commanders. This information, slow and often dated, nevertheless had the potential to give commanders a battlefield advantage. Its value depended on whether the information was correct and used before the enemy could counteract. With computers, the concept of controlling the vast sea of information to one's advantage has become so critical, the U.S. devotes extensive resources to the study and development of IW concepts.⁵

A computer network, and its power to enhance both weapon and non-weapon assets, is a valuable new source of power for the commander. This "tool" increases the quantity, quality and variety of information to the commander and improves performance. Computers also have another power beyond direct military support--computers now directly control large, complex machine systems as well as military and civilian support systems. Modern society and military forces have become extremely dependent on this capability. The shift from the old military-industrial complex to the new military-civilian computer complex forces this increased reliance on automated information as well as blurring the line between military and civilian systems.⁶ Computers have the ability to effectively manage both the highly integrated, enormous battle-space involved in today's campaigns as well as cheaply control the society's machinery and civilian infrastructure supporting these military ends.⁷

The Concepts of Netwar

"The whole thing boils down into control; power in all its forms."

George A. Furse

DOD Directive 4600.4 levies commanders to attack enemy perceptions, decision processes and control mechanisms; in short all aspects of a society--political, economic, and military.⁸

In developing support for this directive, the School of Information Warfare and Strategy at Ft. McNair in Washington perhaps describes the scope of IW best: "While (IW) is ultimately military in nature, IW is also waged in political, economic, and social arenas and is applicable over the entire national security continuum from peace to war and from "tooth to tail".⁹ As a new IW tool, Netwar shows its maximum potential in this "tail" described above. Netwar is conducting offensive and/or defensive operations on military or civilian non-weapons computer networks to gain a military advantage. As with any new facet of warfare, its definition is incomplete and overlaps with other IW definitions and concepts. But, just like the W.W.II propeller-driven aircraft gained potential with the advent of the supercharger, so IW gains new potential through Netwar. In a nutshell, Netwar is tomorrow's computer-based, information-related conflict between either nations, organizations, or societies.

The Toffler's, in their book War and Anti-War, envision the future of American conflicts. They feel societies fight the same way they make money--and as America moves from an industrial to an information economy, DOD will depend more on information dominance.¹⁰ Commanders need to understand this concept and capitalize on the potential of Netwar for computer networks make a critical impact on every facet of military and civilian operations.

Netwar isn't an end, it is merely a means to an end. The goal of Netwar, whether offensive or defensive, is to give the commander an advantage. To do this, Netwar's operational concept focuses on defending friendly computer network assets while exploiting the enemy's. Since resources and time are limited, Netwar planners must also provide the commander with priorities, so he/she can select and use Netwar to maximize its impact on a particular Course Of Action (COA). Additionally, Netwar is not just a wartime operation. It must be conducted in peacetime to prepare the battlefield for a possible engagement and, much like peacetime intelligence activities, help the commander prepare for or possibly avert conflict. Not only is the West worried--Russia's President Yeltsin and Defense Minister Kokoshin have repeatedly written and spoken about their concerns over potential enemy action on their

information systems.¹¹ China, Israel, Australia, Germany, and Canada have followed Russia's lead and are all very busy enhancing systems and building emerging Netwar strategies.¹²

In offensive Netwar, the commander seeks dominance over the enemy's computer information and control systems using a myriad of tools. The commander can attack either the physical computer network, its supporting structure, or a product of the network. The attack mode can be overt or covert and consists of either a hard or soft kill. It can directly impact the immediate battle or affect the enemy commander's conduct of future engagements.

Defensive Netwar helps the commander get "trusted" information by protecting computer hardware and its infrastructure; providing secure communication links and when required, an encryption/decryption capability. Defensive Netwar also depends on "reliable" soft and firmware, and an ability to detect, correct and/or recover from attacks. "Trusted" information is the goal, but when "trust" is violated, defensive Netwar must notify the commander and provide him/her with alternate means of gaining "trusted" information again.

Netwar is not "bloodless" warfare as envisioned by some futurists.¹³ With other tools, it may help avert a conflict by putting the enemy at a real or perceived disadvantage, or perhaps lessen casualties by providing swifter means to victory--but it is not a panacea. Also, Netwar can neither defeat all networks nor defend against all attacks. However, effective offensive Netwar can significantly decrease the enemy's confidence in their information or allow the friendly commander to manipulate the enemy; while effective defensive Netwar can protect friendly assets and increase the reliability of friendly information.

Netwar at the Operational Level

"Gen. Schwarzkopf generated only a tenth of the total message traffic."

Signal Magazine

Netwar holds tremendous power for the commander, as well as tremendous potential for disaster. In Desert Storm, the "brilliant" IW successes for the coalition overshadowed two critical elements that won't exist in future conflicts. First, time allowed the coalition to find serious network deficiencies and fix them. Second, and most critical, Iraq did not use Netwar because it lacked effective technology and strategy. This lack of Iraqi action and its

consequences are lessons that won't be lost on future adversaries. Just as the coalition learned from Desert Storm, new foes are also "going to school" to avoid the Iraqi disaster.

The commander must plan for possible Netwar action in every COA, even in light of an apparently unsophisticated enemy. Netwar, especially offensive Netwar, is a skill that is easily "hired" by a potential adversary.¹⁴ It doesn't take tremendous capital or complicated machinery--Robert Morris, a hacker, brought down a 7,000 unit "secure" American system with an Apple IIe and a 1200 baud modem.¹⁵ Commanders must prepare for effective defenses against Netwar during peacetime and practice those plans, regardless of the foe's Netwar "readiness". But, Netwar is not just hooking up a PC to a telephone and frying computers or wreaking havoc with a power-grid. Netwar, if not properly handled, can have unintended and severe consequences.¹⁶ Planning must be centralized and coordinated at the operational level. Decentralized planning could lead to disaster for the friendly forces.

The Realities about Computers and Networks

On 15 January 1990, 50% of AT&T's long distance switching system died--due to 13 lines of hacker code. It took 9 hours to pour through millions of lines of code before the problem was solved.

Law And Disorder on the Electronic Frontier

Commanders must face reality--any computer-controlled system can be affected. The concept of an "impenetrable" system is a mirage. For example, in the 1980's, a hacker defrauded a major U.S. bank of millions by simply cutting thin "salami slices" from millions of daily bank transactions.¹⁷ This activity was conducted on a "100% secure" banking network. If the computer is relatively secure, there are alternatives. Secondary sources--keyboard emissions, CRT radiation, or printer heads striking paper can be intercepted.¹⁸ Something as simple as tertiary "reflective" computer emissions bouncing off innocent hardware (like doorknobs or the neutral wire of a wall outlet) are susceptible to interception.¹⁹

Another reason computer systems are vulnerable is because they are now very complex, requiring constant maintenance. To illustrate, software developed for the Space Shuttle motor and hydraulic control systems (the Space Shuttle is the world's most complicated mechanical device) has 420,000 lines of code. A simple modern DOD "comm" package needs

1.5 million lines of code.²⁰ These huge programs, just like anything built by humans, have flaws. "High Quality" software may contain one error per 1,000 lines of code.²¹ According to E.W. Dijkstra, a leading U.S. software engineer, testing for bugs "...can only show the presence of bugs, never their absence."²² NORAD and similar sized systems have computer codes with as many as 40,000 errors, yet they are still considered "reliable".²³ To maintain these systems, software is constantly upgraded. This critical maintenance is where planners can easily affect the system and get into a "secure" system. There are also other means, such as remote modem access through an "unsecured server" and hardware manipulation. The bottom line is clear--systems are reachable, the only variables are how much time and resources it takes. The military's "Tempest" systems aren't immune either--Pengo, a West German computer hacker, sold American military secrets to the USSR. He repeatedly broke into Tempest computers at MIT, Jet Propulsion Labs, Union Carbide, Mitre, Redstone, and the Pentagon.²⁴

Netwar Potential: On the Offense

In the first 30 hours of Desert Storm, U.S. troops got 1.3 million electronic messages. "It was overload."
Maj. Gen. Paul K. Van Riper, USMC, assistant chief of staff for C4I

Offensively, Netwar must support the friendly commander's ability to affect the enemy's decision cycle, often referred to as the Observe, Orient, Decide, Act (OODA) Loop. Commanders must develop what Ryan, et. al. describe in their research as an "...information Order of Battle...." defining systems, networks and facilities as to their usefulness as targets; giving them a level-of-effort; and allocating either organic resources or upchanneling requests for resources from other commanders, federal agencies, or even foreign governments.²⁵

First, the commander must determine the goal of offensive Netwar. Goals must be defined before targets or levels-of-effort are selected. *Netwar is not* destroying the enemy's computer systems. *Effective Netwar gives the commander tools* to achieve goals on his "battlefield". When contemplating Netwar, commanders should ensure staffs integrate Netwar goals into overall theater objectives. Offensive Netwar involves intercepting, manipulating, controlling, disrupting, corrupting, or destroying the enemy's information capabilities and/or systems.²⁶

Once goals are determined, the next step is selecting the target and appropriate level-of-effort. Target selection goes well beyond the physical computer system itself--target selection must consider what the computer system actually controls or supports. Just because an enemy computer system is vulnerable does not define it as a worthy target. In future conflicts, the NCA may direct efforts against enemy credit systems, banks, or industrial production; or perhaps control of transportation, gas, power, water and sewage control systems; then targeting the computers that operate those systems becomes an effective use of Netwar.²⁷ Also, indirect targets must be considered. Aside from hardware, firmware, software, input data attacks, and output information manipulation, the people who operate/maintain these systems are viable indirect targets. The foe's automated data processing personnel and support technicians may cooperate with friendly efforts to gain success in Netwar.²⁸ Also, commanders must consider potential targets outside their Area Of Responsibility (AOR). Computers, especially processor chips and network systems, are built by relatively few manufacturers worldwide. If required, commanders must up-channel their needs to senior leadership and they, in turn, should seek help from appropriate agencies. Gaining cooperation from computer makers as they service and/or supply the enemy can go a long way in achieving the commander's goals.²⁹ To illustrate, computer components are now capable of either degrading or completely failing automatically through a simple external command or after a preset array of conditions is met.³⁰

Hand-in-hand with target selection is assigning a level-of-effort. Here, vulnerability and the commander's ability to threaten that vulnerability must match. Commander's must allocate offensive resources only where they have the best chance of achieving needed goals.³¹ Levels-of-effort span from physical destruction to signals interception and modification; to ignoring, modifying, invading, or disrupting either the computer, the network, or its support systems.

The choice of physical action--destroying the computer network, forces the enemy to either act in the blind (as Iraq did) or rely on less sophisticated (and possibly more exploitable) back-up systems.³² But, destruction goes beyond traditional "bombing". Destruction includes

incapacitating internal components, interface systems, communications nodes, and/or affecting support systems such as power supplies and conditioning equipment. Weapons include sound, heat/cold, radar/magnetic energy, and light energy.³³ Additionally, RF weapons, the synchronous pulsing of electromagnetic energy, are particularly effective weapons because they destroy the computer but leave the structure unaffected. At the high end of the RF range is the Electromagnetic Pulse (EMP) created by a nuclear blast. However, a "poor man's" EMP is simply a surge in the computer's power supply. Both are effective.³⁴

When considering physical destruction, commanders must continually look beyond the immediate benefits of such action and create a balance between combat needs and the long term responsibilities during war termination and post-conflict reconstitution. Following a common sense principle of war, Netwar must achieve its goals with the minimum of damage. The systems a commander affects to his/her advantage during the opening shots may be the very systems the commander needs in war termination and post-conflict reconstitution. To cite an old friend of battle theory, Clausewitz continually emphasized the need for commanders to not take the first step until the last step has been contemplated.³⁵ As an example, complete destruction (bombing) of an enemy's communication, banking, and transportation system (when simple degradation would have achieved the intended goal) only makes war termination more difficult. Additionally, it severely affects the defeated foe's ability to reconstitute, adding unnecessarily to post-conflict tensions. Avoiding "overkill" in Netwar is more critical than avoiding unneeded physical destruction in C2W because unlike C2W, which targets primarily military assets, Netwar targets systems that are either shared civil/military systems--or totally civilian resources. Some of these target categories, such as medical and pharmaceutical control systems or computer systems controlling food supplies, transportation systems, public utilities, banking centers and/or certain civilian production facilities are "gray" legal areas. These target categories must be carefully screened by legal advisors.³⁶ Additionally, commanders must assess the legality as well as the cost-to-benefit ratio of attacking these systems as they impact not just the progress of the military campaign, but the effect on

continued political support from the U.S. public, elected representatives, and coalition members. To dramatize this point, destroying a "bar code" data base in the enemy's food production infrastructure may help the friendly commander by disrupting logistics supplies to enemy troops, but if it also creates a CNN news-scoop showing "starving children", the long-term cost in public support may outweigh the immediate military benefit.³⁷

A highly preferred level-of-effort would simply degrade computer systems. By affecting the computer's capabilities to perform consistently, Netwar goals are achievable without physical destruction. This level-of-effort has several positive facets. Commanders can overtly degrade the system; not destroying it, but destroying the enemy's trust in the system's reliability. This has the compounding affect of tainting the enemy's trust in every one of its computer systems, whether or not it was affected by U.S. action. Conversely, the computer may be covertly intruded so the output is altered to the advantage of the U.S. commander, but without the enemy commander's knowledge, thereby retaining the enemy commander's "trust" in a system being manipulated by friendly forces. Included here are voice and data networks. Not only are these high-value, but with over 4,000 telephone companies worldwide, this is a target-rich environment.³⁸ Another level-of-effort option is affecting the enemy's computer output through software and/or input data manipulation; producing plausible outputs for the enemy, but controlled by friendly assets. For example, positioning (modifying radio and television signals), could disrupt the enemy's political power base or governmental control. Envision a TV broadcast showing the enemy "retreating" or "surrendering".³⁹ More "traditional" invasive techniques include software attacks by any of the following means: a Trojan Horse, worm, virus, logic bomb, and/or an Easter Egg (as in Tom Clancy's "Debt of Honor") as well as a trap door.⁴⁰ These hacker "legacies" have a definite value in Netwar.⁴¹

A low-priority target may either be monitored or ignored. When monitoring, a commander uses signals interception and modification to either gain information or deny the enemy its use. For example, rendering an enemy's ciphered transmission useless denies it to the friendly commander, but it does the same to the enemy.⁴² Finally, if a system is low priority, it should

be ignored. Ignoring low-value systems preserves friendly offensive assets while saving those enemy systems for possible reassignment during war termination and reconstitution efforts.

Finally, the idea of information overload has its place in offensive Netwar. Overwhelming systems with fed or perpetual-generating data seeks to either slow down legitimate computer operations, incapacitate the network through gridlock, or cause the human filter receiving the avalanche of output to become ineffective. Overwhelming the enemy gives the commander an advantage; he/she can get around the enemy's OODA Loop faster than the enemy can itself.

Critical to offensive Netwar planning is an emphasis on coordination and effective timing. This is where joint, centralized, and coordinated planning efforts are vital to success. Redundant efforts are inefficient, waste resources, and create unneeded risks. Also, coordination precludes situations where one "friendly" plans to affect a system while another simultaneously requires the use of the same enemy system to achieve its mission goals. In addition to internal coordination, commanders must weigh the cost-to-benefit ratio of allowing coalition partners in on the planning efforts.⁴³ How much information should be shared with coalition partners is a tough issue; a current coalition partner may become tomorrow's foe. A parallel dilemma is what to do with economic enemies who are political friends. As an example, during Desert Storm France made Spot imagery commercially available, even to Iraq.⁴⁴ Smart force planning averted an information disaster on the eve of ground operations. Finally, temporary alliances, such as the Desert Storm coalition with Syria require commanders to consider how much information is shared and what benefit is gained.⁴⁵ The Netwar plan must also emphasize timing. To illustrate, blinding the foe's communications after the enemy used it for its intended purpose is pointless. On the other hand, blinding a system too soon is just as pointless--it gives the enemy time to recover or seek alternate routes for information.⁴⁶ Coordinated, effective timing not only maximizes operational success, but reduces the risk of Netwar "fratricide".

Another facet to Netwar planning is the need for constant peacetime exercises to check validity. Potential COA and enemies must be continually assessed. Opponent's cable

systems, relay towers, telephone switching nodes and exchanges, fiber optic and coaxial cable runs must be continuously updated for location and use.⁴⁷ Potential enemy computer software, firmware, and hardware changes must be monitored to determine status and potential vulnerabilities. This continuous monitoring is critical due to the pace of change in computer technology. Today's Netwar plan can become instantly obsolete as a potential foe upgrades its computer defenses or corrects physical security flaws. These operations should be covert. Active peacetime operations give the commander the power to put systems and options "in place" prior to a conflict. In fact, peacetime Netwar gives the commander options that could prevent war. Well placed logic bombs and latent viruses can threaten the foes' civil and military computer operations if they start action against U.S. interests.⁴⁸

Finally, just like a child who dismantles his dad's radio with no clue on reassembly, reckless Netwar without a plan for post-conflict reconstitution is extremely counter-productive. The goal is to reasonably restore the systems' performance, while retaining the ability to conduct future Netwar action if needed. To reconstitute every affected enemy computer after a large scale action would take more work than resources allow. Therefore, planners must prioritize which systems get restored and to what level. To meet this goal efficiently, pre-conflict planning must include documentation of all friendly "attack" actions, leaving an audit trail for the reconstruction engineers to follow. Also, the concept of achieving goals with minimum damage to the enemy's systems will significantly ease the reconstitution effort. Basic service systems (communications, power, gas, water, sewer, and transportation) should receive top priority, they should either be restored or (if physically destroyed in war) replaced. Secondary efforts should rebuild the economy (banking systems, production and inventory systems) as well as internal security. Replacement and restoration presents the U.S. commander with a unique opportunity to configure the reconstituted system(s) to his/her advantage for a future potential Netwar option--this valuable tool should not be overlooked.

Netwar on the Defense

"Hackers from Denmark, Russia, and Iraq tried to penetrate Desert Storm military computer systems."

William Matthews, news correspondent

An attack on U.S. computer systems is "assured" during the next conflict--with high probability of "hits" on both the "secured" systems and less defended support computer systems.⁴⁹ Effective defense requires an assessment of the friendly systems' vulnerabilities as well as the enemy's potential to threaten that vulnerability.⁵⁰ If both conditions exist, and the system is vital, commanders must protect it.⁵¹ There is a tradeoff with security--commanders must accept inefficiencies with high security levels; compartmentalized data and/or computers are relatively tight, but slower than comparable "unsecured" systems.⁵² They must also guard against computer security discipline sliding during the heat of battle as workers rush to gather critical information.⁵³ Regardless of human frailty under fire, planning for defensive Netwar must proceed and include four levels: prevention, detection, limitation, and recovery.⁵⁴ Finally, defensive Netwar must be coordinated with C2W defensive efforts--the two are closely linked on defensive efforts and can easily share vital resources and options.

Prevention is first. It involves the physical layout and construction/composition of the computer facilities, including modulated power or Uninterruptable Power Supply (UPS); its supporting computer security architecture; as well as the internal policies implementing the preventative measures. When planning defensive Netwar, security must also extend to the entire system, not just to the command section. To illustrate, Saudi Arabia, had a limited secure network infrastructure. The first Defense Satellite Communications System dish in Saudi Arabia was bolted on the roof of the Saudi Defense Ministry building with cables running down the outside walls. Although armed guards protected against unauthorized physical access to the building, the cable radiated sensitive communication signals--an easily intercepted source.⁵⁵

Operational security may require data encryption. Though encryption has obvious benefits, there are costs and risks. First, encryption/decryption uses sophisticated equipment,

can only be performed at specified sites, and consumes vital resources. Also, encryption indirectly alerts the enemy that you have something worth hiding. This makes encryption assets priority targets for disruption, interception, or destruction. Also, encryption personnel are at risk--requiring a higher level of personnel security for these vital human resources. Prevention may also use a trusted third-party to audit usage and hard-copy (notarize) each access. Hard-copy audit trails also make recovery work easier--most unauthorized break-ins have with them a clean-up device that erases any electronic audit trail.⁵⁶

Surprising to some, but many "secure" systems are invaded not because security is defective, but because operators do not use it. From "dumpster diving" for ID/Password keys, to leaving secure components unsecured, to connecting unsecured components to secure devices, to deliberately disabling security features to save time--security breaches are a people problem as much as a systems issue. A Defense Information Systems Agency study claimed that effective human defensive actions could prevent/detect 80% of illegal computer "hits".⁵⁷ Security items like dial back, ID/Password requirements, data file password protection, file access restriction, and third party ID authentication & verification are useless if not consistently applied or if purposely circumvented. When allocating resources for physical security, the commander would be wise to follow commercial sector security examples. Major corporations spend up to 68% of their security budget on education, not hardware.⁵⁸ Recent USAF conferences on IW have emphasized the criticality of proper training and education. This emphasis directly reflects the security concerns of the USAF's chief trainer, Gen. Henry Viccellio Jr., Commander, Air Education and Training Command.⁵⁹ This education must involve not only U.S. DOD personnel, but U.S. government workers and contractors as well as coalition and allied personnel. The following illustrates the lack of physical security training and education. During Desert Storm, in the Saudi AOR, 3,000 personal computers were connected to the U.S. mainland via network, with many connections made "...outside the security envelope, creating an enormous exploitation risk."⁶⁰ Coalition forces were lucky, because these opportunities were lost by Iraq--opportunities the next foe

will not pass up.⁶¹ Although operational commanders are not directly involved in these training issues, they must continually assess their force's "Netwar readiness" and relay training needs back to the supporting commanders. To illustrate, Gen. Dwight Eisenhower was so hampered by a lack of skilled radio intercept and deciphering experts, he physically created a specialty within the Army Signal Corps to address this WWII version of IW.⁶² Finally, commanders must also weigh security risks against operational rewards when developing networks with hastily organized coalitions--like the U.S. did in Desert Storm.⁶³

Next, detection is critical for maintaining the commander's "trust" in the information. If a system is tampered with, friendly forces must know the output information is probably corrupt and must either work without that data or seek alternate information paths. Systems with a baseline can perform automatic or directed comparison checks (parity checks) to detect fraudulent operations.⁶⁴ Another prevention measure includes a system that continuously monitors or "snoops" for unauthorized hits.⁶⁵ The sensitivity of these monitors is adjustable and customized to meet the threat. These "snooping" programs are programmed to alert only after a predetermined set of trigger events or flags occur, but these security applications only work if applied.⁶⁶ Slack application of parity checks at the General Electric Missile & Space Division in Valley Forge PA compromised sensitive DOD information. The same can be said for NORAD operations during periods in the 1980's.⁶⁷

Another detection issue is handling stimuli, or induced information overload. It can render a computer stupid, or cause significantly degraded performance. Thus the coalition OODA Loop is slowed, forcing potentially bad decisions.⁶⁸ Here, the commander counters with "sniffers" that detect/counter stimuli before it overwhelms.⁶⁹ Another defensive strategy that increases the commander's "trust" is setting up parallel systems with different hard/software and communications circuits as well as unlike operating systems (Apple System 7 parallel with a DOS system).⁷⁰ This significantly complicates an enemy's tampering efforts.

If detection spots who is getting inside a computer system, limitation (firewalls) seeks to restrict the amount of movement available once inside. Commanders must stick to tough

compartmentalization of sensitive operations, even if it causes operational inefficiencies. Also, isolating highly-sensitive computer assets from networks either permanently or when not actively engaged in network operations increases the system's integrity.

Finally, recovery provides the commander a way to reconstitute operations after the inevitable enemy attack. Recovery is a mandatory part of defensive Netwar. Commanders that ignore this vital fallback position will pay the penalty in future conflicts. Recovery may entail off-site data and/or computing back-up; special recovery software designed to rebuild lost, damaged or deleted files; or emergency (manual) information back-up systems that aren't dependent on computers for control or execution. Commanders can appreciate the need for recovery after considering that over 95% of DOD telecom (voice and data) is provided by public networks owned by common carriers. When the National Information Infrastructure is completed, it will use these same utilities.⁷¹

Recommendations and Conclusion

"The services put more electronic communications connectivity into the Gulf in 90 days than we put in Europe in 40 years."

Lt. Gen. James S. Cassidy, director of C3 for JCS

There is a danger in using Desert Storm as the defining moment for future IW. Before the U.S. grabs this one experience as the foundation for advanced IW operations, the U.S. must understand that Desert Storm was unique. U.S. operational commanders must now plan to "...dominate the entire information spectrum," while our enemy does the same.⁷² Netwar helps the commander achieve domination of the "entire" spectrum. Netwar takes IW deeper into the enemy's homeland and risks more and more of its assets. Those who cling to Clausewitz's concept of the limited role of technology need to consider its context. He wrote when major technical revolutions occurred once every 50 to 100 years. We live in an age when there is potential for major change every 24 months.⁷³ To ignore offensive and defensive Netwar gives the enemy an advantage that cannot be made up for in battle. To cite George A. Furse, "Let it not be supposed that there is some occult means by which neglect in peace could be atoned for in war."⁷⁴

Netwar also requires a new organizational paradigm. To fit this new tool into an established way of operations could invite disaster. Much like the French failure to adapt the machine gun in WWI, Netwar requires a modified structure.⁷⁵ Netwar requires centralized planning and "top-sight" to ensure the assets are effectively used.⁷⁶ During planning, this level of supervision is needed because of the extreme sensitivity of Netwar. For several of the target options, NCA approval may be needed. However, the actual execution must be decentralized to the "shooters" at the keyboards and troop level so that the plan can maintain flexibility during its hectic execution. Unlike Vietnam, where technocrats kept both command and execution at ridiculously high levels, Netwar commanders must plan and coordinate, then let go of the reins.⁷⁷ Desert Storm offers a good comparison of the genesis of Netwar planning and execution. Instead of a stovepipe, C2W (the "sister" to Netwar) used a flat, inter-dependent organization where problems were discovered in Saudi; solutions developed and coordinated stateside between military experts and civilian contractors; then corrective action taken by defense logisticians over 7,000 miles from the desert.⁷⁸

Netwar is a "growth industry". Defense Information Systems Agency estimates over 900,000 illegal "hits" occurred in 1991 on federal computers--up from 395,000 in 1989.⁷⁹ This threat needs its own expertise base, much like Eisenhower's radio cadre. However, to predict the precise future of Netwar and the demands it places on DOD is impossible; to project trends is a bit easier. American society will continue to embrace technology, both its good and bad sides. The military will naturally be drawn along on this trend, and as the civilian/military network delineation becomes more and more blurred, America can anticipate increasing vulnerability to Netwar. Failure of the operational commander to anticipate, prepare for and execute Netwar will cost the commander the use of a valuable force enhancer.

Notes

Fiber optics were touted as "spook-proof". Even fiber optic lines can now be tapped.

Law And Disorder on the Electronic Frontier

- ¹Arquilla, John and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy, April-June 1993, p. 149.
- ²Furse, George A., Information in War: Its Acquisition and Transmission. (London: William Clowes & Sons, Ltd., 1985), p. 29.
- ³Macedonia, Michael R., "Information Technology in Desert Storm", Military Review, October 1992, p. 35.
- ⁴Telephone conversation with Gregge E. Haege, Major, USAF, Headquarters Air Education and Training Command, Technical Training Directorate, Randolph, AFB, 1 May 1995.
- ⁵Ibid.
- ⁶Mathews, William, "New School to Focus on Information Warfare," America On-Line Download from Army Times Publishing Company, July 18, 1994.
- ⁷McAfee, John and Colin Haynes, Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System: What They are, How They Work, and How To Defend Your PC, Mac, or Mainframe (New York, St. Martin's Press, 1989), p. 190.
- ⁸Hutcherson, Norman B., Command & Control Warfare (Maxwell AFB: 1994), p. 15.
- ⁹Geissler, Fred, Introduction to Information-Based Warfare (Washington, D.C., School of Information Warfare, March 1995), p. 34.
- ¹⁰Toffler, Alvin and Heidi, War and Anti-War: Survival at the Dawn of the 21st Century (New York: Bantam Books, 1993), p. 3.
- ¹¹Fitzgerald, Mary C., "Russian Views On Electronic Signals and Information Warfare," American Intelligence Journal, Spring/Summer 1994, p. 87.
- ¹²Contract no. DCA 100-90-C-0058, Planning Considerations for Defensive Information Warfare-Information Assurance, Task Order 90-SAIC-019 (Alexandria, VA: 1993), p. 17.
- ¹³Ryan, Julie and Gary Federici, Offensive Information Warfare--A Concept Exploration. (Alexandria, VA: 1994), p. 4
- ¹⁴Busey, James B., "Information Superiority Dashes Thorny Power Projection Issues," Signal, November 1994, p. 13.
- ¹⁵Hafner, Katie and John Markoff, Cyberpunk: Outlaws and Hackers on the Computer Frontier. (New York: Simon and Schuster, 1991), p. 302.
- ¹⁶Center for Naval Analysis, Checkmate 2010 Information Warfare: A Policy and Technical Prospect. (Alexandria, VA:1993), p. 4
- ¹⁷U.S. Dept. of Commerce, Computers: Crimes, Clues and Controls (Washington, D.C.: 1987), p. 11.
- ¹⁸The Military Frontier: Understanding Computers. (Alexandria, VA: Time-Life Publishers, 1991), p. 104.

¹⁹Metzar, Terry, "Hostile Intercepts Aimed At Information Systems," National Defense, May-June 1993, p. 25.

²⁰Ramstad, Evan, "Risky Business," The Newport (RI) Daily News, 8 April 1995, p. C7.

²¹Bellin, David and Gary Chapman, eds., Computers in Battle, Will They Work? (Boston: Harcourt Brace Jovanovich, 1987), p. 223.

²²*Ibid.*, p. 222.

²³*Ibid.*, p. 225.

²⁴Hafner, p. 185.

²⁵Ryan, Julie, Gary Federici, and Tom Thorley, Information Support to Military Operations in the Year 2000 and Beyond: Security Implications (Alexandria, VA: Center For Naval Analysis, 1993), p. 12.

²⁶Telephone conversation with Gregge E. Haege.

²⁷Parker, Donn B., Crime by Computer (New York: Scribner, 1976), p. 258.

²⁸*Ibid.*, p. 238.

²⁹*Ibid.*, p. 260.

³⁰Telephone conversation with Richard W. Griffith, Defense Computer Contractor, Shreveport, LA, 5 May 1995.

³¹*Ibid.*

³²Arquilla, p. 157.

³³U.S. Dept. of Commerce, Computers: Crimes, Clues and Controls, p. 27.

³⁴Ryan, Julie and Gary Federici, p. 6.

³⁵Clausewitz, Carl von, On War, Translated and edited by Sir Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), p. 263.

³⁶Center for Naval Analysis, Checkmate 2010 Information Warfare: A Policy and Technical Prospect, p. 4.

³⁷Parker, Donn B., Crime by Computer, p. 268.

³⁸Sterling, p.176.

³⁹Center for Naval Analysis, Checkmate 2010 Information Warfare: A Policy and Technical Prospect, p.4.

⁴⁰Clancy, Tom, Debt of Honor (New York: G.P. Putnam's Sons, 1994), p. 288.

⁴¹Ryan, Julie and Gary Federici, p. 4.

⁴²Davies, D.W. and W.L. Price, Security for Computer Networks (New York: John Wiley and Sons, Inc., 1984), p. 11.

-
- ⁴³Pudes, Terry J., "Preparing Future Coalition Commanders," Joint Forces Quarterly, Winter 1993-1994, p. 2.
- ⁴⁴Ryan, Julie, Gary Federici, and Tom Thorley, p. 12.
- ⁴⁵Ibid., p. 18.
- ⁴⁶Emmett, P.C., "Software Warfare: The Emerging Future," RUSI Journal, December 1992, p. 58.
- ⁴⁷Contract no. DCA 100-90-C-0058, p. 22.
- ⁴⁸Lind, William s., Kieth M. Nightengale, Scott Schmitt, Joseph W. Sutton, and G.I. Wilson, "The Changing Face of War Into the Fourth Generation," Military Review, October 1989, p. 7.
- ⁴⁹Busey, James B., "Information Warfare Calculus Mandates Protective Actions," Signal, October 1994, p. 15.
- ⁵⁰Telephone conversation with Richard W. Griffith.
- ⁵¹Contract no. DCA 100-90-C-0058, p. 23.
- ⁵²Telephone conversation with Richard W. Griffith.
- ⁵³The Military Frontier: Understanding Computers, p. 103.
- ⁵⁴U.S. Dept. of Commerce, Computers: Crimes, Clues and Controls, p. 3.
- ⁵⁵Grier, Peter, "The Data Weapon," Government Executive, June 1992, p. 21.
- ⁵⁶Contract no. DCA 100-90-C-0058, p. 49.
- ⁵⁷Ibid., p. 24.
- ⁵⁸Mandron, Thomas W., Network Security in the 90's (New York: John Wiley & Sons, Inc., 1992), p. 223.
- ⁵⁹Telephone conversation with Gregge E. Haege.
- ⁶⁰Grier, p. 21.
- ⁶¹Telephone conversation with Richard W. Griffith.
- ⁶²Hutcherson, p. 21.
- ⁶³Ryan, Julie, Gary Federici, and Tom Thorley, p. 3.
- ⁶⁴Emmett, p. 59.
- ⁶⁵Robinson, Clarence A., "Software Security Protection for Work Stations, Laptop Data," Signal, October, 1994, p. 20.
- ⁶⁶Telephone conversation with Richard W. Griffith.
- ⁶⁷Caroll, John M., The Third Listener (New York: E.P. Dutton and Co., Inc., 1969), p. 12.
- ⁶⁸Ryan, Julie and Gary Federici, p. 9.

⁶⁹Telephone conversation with Richard W. Griffith.

⁷⁰Contract no. DCA 100-90-C-0058, p. 40.

⁷¹Ibid., p. 42.

⁷²Campen, Alan D., First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf (Fairfax, VA: AFCEA International Press, 1992), p. 20.

⁷³Emmett, p. 57.

⁷⁴Furse, p. 98.

⁷⁵Arquilla, p. 151.

⁷⁶Hutcherson, p. 7.

⁷⁷Mathews, William, "Girding for Cyberwar," America On-Line Download from Army Times Publishing Company, Washington, D.C., 18 July 1994, p. 1.

⁷⁸Arquilla, p. 152.

⁷⁹Robinson, p. 19.

BIBLIOGRAPHY

1. Arquilla, John and David Ronfeidt. "Cyberwar is Coming!" Comparative Strategy, April/June 1993, p. 141-165.
2. Bellin, David and Chapman, Gary, eds. Computers in Battle, Will They Work? Boston: Harcourt Brace Jovanivich, 1987.
3. Benedikt, Michael, ed. Cyberspace: First Steps. Cambridge: MIT Press, 1991.
4. Busey, James B. "Information Warfare Calculus Mandates Protective Action." Signal, October 1994, p. 15.
5. _____. "Information Security Dashes Thorny Power Projection Issues." Signal, November 1994, p. 13.
6. _____. "Let Loose the Dogens of Cyberspace." Signal, April 1995, p. 13.
7. Campen, Alan D. "Information Warfare is Rife with Promise, Peril." Signal, November 1993, p. 19-20.
8. _____. First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf. Fairfax, VA: AFCEA International Press, 1992.
9. _____. "Information is Rife With Promise, Peril." Signal. November, 1993.
10. Carroll, John M. The Third Listener. New York, E.P. Dutton and Co., Inc., 1969.
11. Center for Naval Analysis. Checkmate 2010 Information Warfare: A Policy and Technical Prospect. Alexandria, VA: 1993.
12. Clancy, Tom. Debt of Honor. New York: G.P. Putnam's Sons, 1994.
13. Clausewitz, Carl von. On War. Translated and edited by Sir Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.
14. Computers: Crimes, Clues and Controls. U.S. Federal Government Doc, Washington DC: 1991.
15. Davies, D.W. and W.L. Price. Security for Computer Networks. New York: John Wiley and Sons, Inc., 1984.
16. Emmett, Flt. Lt. P.C. "Software Warfare: The Emerging Future." RUSI Journal, December 1992, pp. 56-60.

17. "Evolving The National Information Infrastructure (NII)". Naval War College Symposium for Government and Industry: Newport, RI, 9 January 1995.
18. FitzGerald, Mary C. "Russian Views On Electronic Signals and Information Warfare." American Intelligence Journal, Spring/Summer 1994, pp. 81-87.
19. Furse, George Armand. Information in War: Its Acquisition and Transmission. London: William Clowes & Sons, Ltd., 1985.
20. Geissler, Dr. Fred. Introduction to Information-Based Warfare. Alexandria, VA: School of Information Warfare and Strategy Symposium, 20-24 March 1995.
21. Gordon, Michael R. "Admiral With High-Tech Dreams Has Pentagon at War With Itself." The New York Times, 12 December 1994, p. A-17.
22. Grier, Peter. "The Data Weapon." Government Executive, June 1992, pp. 23-26.
23. Hafner, Katie and Markoff, John. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon & Schuster, 1991.
24. Higinbotham, James H. et al.. Doing Deception: Attacking the Enemy's Decision Processes. Alexandria, VA: February 1990.
25. Hudson, Neff. "Future Shock." Air Force Times, October 25, 1993, p. 19.
26. Hutcherson, Lt. Col. Norman B. Command & Control Warfare. Unpublished Research Paper, Air University, Maxwell AFB, AL: 1994.
27. Koch, Maj. James R. "Operation Fortitude: The Backbone of Deception." Military Review, March 1992, p. 66-77.
28. Landreth, Bill and Reingold, Howard. Out of the Inner Circle: A Hacker's Guide to Computer Security. Bellevue, WA: Microsoft Press, 1985.
29. LaQuey, Tracy L. and Ryer, Jeanne C. The Internet Companion: A Beginner's Guide to Global Networking. Reading, MA: Addison-Wesley, 1992.
30. Leichter, William E. The Revolution in Military Affairs And Information Warfare. Unpublished Research Paper, U.S. Naval War College, Newport, RI: June 1995.
31. Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Unpublished Research Paper, National Defense University, Washington D.C.: 1994.
32. Lind, William S., Keith M. Nightengale, Scott Schmitt, Joseph W. Sutton, and G. I. Wilson. "The Changing Face of War Into the Fourth Generation." Military Review, October 1989, p. 2-11.

33. Luoma, William M. "Netwar: The Other Side of Information Warfare." Unpublished Research Paper, U.S. Naval War College, Newport R.I., June 1994.
34. Macedonia, Maj. Michael R. "Information Technology in Desert Storm." Military Review, October 1992, p. 34-41.
35. Mandron, Thomas W. Network Security In The 90's. New York: John Wiley and Sons, Inc., 1992.
36. Mathews, William. "New School to Focus on Information Warfare." America On-Line Download from Army Times Publishing Company, Washington, 18 July 1994.
37. _____. "Girding for Cyberwar." America On-Line Download from Army Times Publishing Company, Washington. July 18, 1994.
38. McAfee, John and Haynes, Colin. Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System: What They are, How They Work, and How To Defend Your PC, Mac, or Mainframe. New York: St. Martins' Press, 1989.
39. Metzgar, Terry. "Hostile Intercepts Aimed At Information Systems." National Defense, May/June 1993, p. 24-26.
40. Parker, Donn B. Crime by Computer. New York: Scribner, 1976.
41. _____. Fighting Computer Crime. New York: Scribner, 1983.
42. Planning Considerations for Defensive Information Warfare. Task Order 90-SAIC-019: Contract #100-90-COO58 DISA, 16 December 1993.
43. Pudas, Terry J. "Preparing Future Coalition Commanders." JFQ, Winter 1993-94, p. 40-46.
44. Ramstad, Evan. "Risky Business." Newport (RI) Daily News, 8 April 1995, p. C7.
45. Robinson, Clarence A. "Software Security Protects Workstations, Laptop Data." Signal, October 1994, p. 19-22.
46. Ryan, Julie, Gary Federici, and Tom Thorley. Information Support to Military Operations in the Year 2000 and Beyond: Security Implications. Alexandria, VA: Center for Naval Analyses, November 1993.
47. _____ and Gary Federici. Offensive Information Warfare--A Concept Exploration. Alexandria, VA: Center for Naval Analyses: July 1994.
48. Sokol, Maj. Joseph, Jr. Counter-Deception, the Commander's Responsibility. Unpublished Research Paper, Naval War College, Newport, RI: June 1993.

49. Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York: Bantam Books, 1992.
50. Stoll, Clifford. The Cuckoo's Egg: Tracking a spy Through the Maze of Computer Espionage. New York: Doubleday, 1989.
51. Telephone conversation with Gregge E. Haege Major, USAF, Headquarters Air Education and Training Command, Randolph AFB, TX. 1 May 1995.
52. Telephone conversation with Richard W. Griffith, Defense Computer Contractor, Shreveport, LA. 5 May 1995.
53. The Military Frontier: Understanding Computers. Alexandria, VA: Time-Life, 1991.
54. Toffler, Alvin and Heidi. Powershift. New York: Bantam Books, 1990.
55. _____. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Bantam Books, 1993.
56. Wylie, Joseph C. Military Strategy: A General Theory of Power Control. Rutgers: The State University, 1967.